

Refined Upper Bounds on Stopping Redundancy of Binary Linear Codes

Yauhen Yakimenka, Vitaly Skachek

Institute of Computer Science

University of Tartu, Estonia

Emails: { yauhen, vitaly } @ut.ee

Abstract—The l -th stopping redundancy $\rho_l(\mathcal{C})$ of the binary $[n, k, d]$ code \mathcal{C} , $1 \leq l \leq d$, is defined as the minimum number of rows in the parity-check matrix of \mathcal{C} , such that the smallest stopping set is of size at least l . The stopping redundancy $\rho(\mathcal{C})$ is defined as $\rho_d(\mathcal{C})$. In this work, we improve on the probabilistic analysis of stopping redundancy, proposed by Han, Siegel and Vardy, which yields the best bounds known today. In our approach, we judiciously select the first few rows in the parity-check matrix, and then continue with the probabilistic method. By using similar techniques, we improve also on the best known bounds on $\rho_l(\mathcal{C})$, for $1 \leq l \leq d$. Our approach is compared to the existing methods by numerical computations.

Index Terms—Binary erasure channel, iterative decoding, low-density parity-check codes, stopping redundancy, stopping sets.

I. INTRODUCTION

Stopping sets are a known cause of failures of message-passing decoders, when applied to binary linear codes on a binary erasure channel [1]. Small stopping sets are especially harmful, as they have higher probability of causing the damage. Stopping sets, however, are determined by the selection of a parity-check matrix of the code, rather than by the code itself. The size of the smallest stopping set is called the *stopping distance* of the corresponding parity-check matrix.

It is observed in [2] that by adding redundant rows to the parity-check matrix, the small stopping sets can be eliminated, i.e. the resulting matrix does not contain stopping sets of small size. On the other hand, the increased number of the redundant rows in the parity-check matrix leads to growth in the decoding complexity. Therefore, generally, the trade-off between the size of the smallest stopping set, and the number of rows in the parity-check matrix, is of significant interest.

More specifically, let \mathcal{C} be a binary linear $[n, k, d]$ code, and let H be a parity-check matrix for this code. Denote $[n] \triangleq \{1, 2, \dots, n\}$. Let $\mathcal{S} \subseteq [n]$ be a set of columns of H . Denote by $H_{\mathcal{S}}$ the submatrix of H , composed from the columns of H indexed by \mathcal{S} .

Definition 1. The set \mathcal{S} is a stopping set in H if $H_{\mathcal{S}}$ contains no row of Hamming weight one.

This work is supported by the Norwegian-Estonian Research Cooperation Programme under the grant EMP133, by the Estonian Ministry of Education and Research through the research grants PUT405 and IUT2-1, and by the European Regional Development Fund through the Estonian Center of Excellence in Computer Science, EXCS. The work of the first author is also supported by the HITSA Tiger University programme.

Definition 2 ([3]). The stopping redundancy of \mathcal{C} , $\rho(\mathcal{C})$, is the smallest number of rows in any parity-check matrix of \mathcal{C} , such that the corresponding stopping distance is d .

Bounds on stopping redundancy of binary linear codes were studied in a number of works over the years [3]–[10]. Algorithms for finding small stopping sets were proposed in [11], [12].

For general binary linear codes, the best known bounds on the stopping redundancy were derived by using probabilistic method in [9]. In this work, we improve on the analysis therein. In particular, we observe that the number of stopping sets eliminated by a random codeword of the dual code is not optimal in general case. In our approach, we judiciously select the first few rows in the parity-check matrix, in such way that these rows eliminate more small stopping sets than the randomly chosen nonzero codewords in the dual code. In particular, we pick dual codewords of the minimum weight. If the number of such codewords is small (for example, 1 or 2), then we can provide good estimates on the number of eliminated stopping sets. After that, we proceed with the probabilistic method, similarly to [9].

II. GENERAL THEOREM

Throughout the remaining sections, if not explicitly stated otherwise, we consider a binary linear $[n, k, d]$ code \mathcal{C} . As it was shown in [3, Theorem 3], if $d \leq 3$ then any parity-check matrix H for \mathcal{C} has stopping distance d , i.e. $\rho(\mathcal{C}) = n - k$. Hence we only consider a case $d \geq 4$ (and, therefore, $r \triangleq n - k \geq 2$).

The dual code of \mathcal{C} is denoted by \mathcal{C}^\perp , its dimension and minimum distance are r and d^\perp , respectively. We use \mathcal{C}_0^\perp as a shorthand for $\mathcal{C}^\perp \setminus \{0\}$.

We call any subset of $[n]$ of cardinality i an i -set. The set of all i -sets is denoted by \mathcal{I}_i :

$$\mathcal{I}_i = \{\mathcal{S} \subseteq [n] : |\mathcal{S}| = i\}.$$

We also use the notation $\mathcal{I} = \bigcup_{i=3}^{d-1} \mathcal{I}_i$. We do not consider the i -sets of sizes 1 and 2. Indeed, if $d \geq 4$ then no parity-check matrix has the all-zero column or two identical columns, which implies there are no stopping sets of sizes 1 and 2.

We say that a row vector $\mathbf{h} \in \mathbb{F}_2^n$ covers the i -set \mathcal{S} if the projection of \mathbf{h} on the coordinates indexed by \mathcal{S} has Hamming weight 1. We also say that the $t \times n$ matrix $(\mathbf{h}_1^\top, \mathbf{h}_2^\top, \dots, \mathbf{h}_t^\top)^\top$

over \mathbb{F}_2 covers \mathcal{S} if any of its rows covers \mathcal{S} . If some i -set is covered, then the stopping set in the corresponding coordinates cannot exist. Thus, by covering all the i -sets, $i = 3, 4, \dots, d-1$, we obtain a matrix with no stopping sets of size less than d .

The following lemma is implicitly stated in [9].

Lemma 1. *Let $r \geq 3$ and d be two positive integers, and b be a real number, such that $1 \leq b \leq r-2$, and $(r-1)(d-1) \leq 2^{d-1}$. Then, for any $x < 2^r$,*

$$b - \left(\frac{2^r - 2^{r-b}}{2^r - x} \right) \leq b \left(1 - \frac{(d-1) \cdot 2^{r-d+1}}{2^r - x} \right).$$

We omit the proof of Lemma 1. Next, we formulate a general theorem, which is the main result of this paper. It includes Theorem 7 in [9] as a special case, and its proof uses similar ideas.

Theorem 1. *Assume that there exists a matrix, whose rows $\mathbf{h}_1, \mathbf{h}_2, \dots, \mathbf{h}_\tau$, $\tau \geq 0$, are linearly independent codewords in \mathcal{C}_0^\perp . For $i = 3, 4, \dots, d-1$, let \mathcal{U}_i , $|\mathcal{U}_i| \leq u_i$, be the set of i -sets not covered by this matrix. Assume also that $(r-1)(d-1) \leq 2^{d-1}$. Then*

$$\rho(\mathcal{C}) \leq \tau + \min_{t \geq r} \{t + \kappa_t\}, \quad (1)$$

where

$$\begin{aligned} \kappa_t &= \min \{k \in \mathbb{N} : Q_k(\lfloor \mathcal{D}_t \rfloor) = 0\}, \\ Q_k(x) &= P_k(P_{k-1}(\dots P_1(x) \dots)), \\ P_j(x) &= \left[x \left(1 - \frac{(d-1) \cdot 2^{r-d+1}}{2^r - (\tau + t + j)} \right) \right], \\ \mathcal{D}_t &= \sum_{i=3}^{d-1} u_i \prod_{j=\tau+1}^{\tau+t} \left(1 - \frac{i \cdot 2^{r-i}}{2^r - j} \right) \\ &\quad + \frac{1}{2^{t-r}} \left(1 + \frac{2/3}{2^{t-r+1} - 1} \right). \end{aligned}$$

Proof: Let H be a matrix with rows in \mathcal{C}_0^\perp . Such H is not necessary the parity-check matrix, since its rank can be less than r . Define $\delta(H)$ as follows:

$$\delta(H) \triangleq \left| \{ \mathcal{S} \in \mathcal{I} \mid \mathcal{S} \text{ is not covered by } H \} \right| + (r - \text{rank } H).$$

Here $\delta(H) = 0$ means that $\text{rank } H = r$ and all the i -sets, $i = 3, 4, \dots, d-1$, are covered. Such H is a parity-check matrix of \mathcal{C} , and since its stopping distance is at least 4, all the 1-sets and 2-sets are covered automatically. In the sequel, we construct a matrix H , such that $\delta(H) = 0$.

We prove this theorem in two steps. First, we show existence of a parity-check matrix of size $(\tau + t) \times n$ with bounded δ . Second, we show that δ has to decrease after adding one carefully selected additional row to it. Therefore, after adding enough rows, we obtain a parity-check matrix H with $\delta(H) = 0$. Hereafter, we use H_{i_1, i_2, \dots, i_s} as a shorthand for the matrix with rows $\mathbf{h}_{i_1}, \mathbf{h}_{i_2}, \dots, \mathbf{h}_{i_s}$.

Step 1. Let $\mathbf{h}_{\tau+1}, \mathbf{h}_{\tau+2}, \dots, \mathbf{h}_{\tau+t}$ be t rows drawn uniformly at random without repetitions from $\mathcal{C}_0^\perp \setminus \{\mathbf{h}_1, \mathbf{h}_2, \dots, \mathbf{h}_\tau\}$. Denote by ξ the number of sets in \mathcal{I} that are not covered by $H_{1,2,\dots,\tau+t}$. This ξ is an integer discrete

random variable. Denote by $\mathbf{l}\{\cdot\}$ an indicator function, which takes values 0 and 1. The value of the indicator is set to 1 if the argument is true, and zero otherwise. Then, ξ can be written as follows.

$$\begin{aligned} \xi &= \sum_{\mathcal{S} \in \mathcal{I}} \mathbf{l}\{\mathcal{S} \text{ is not covered by } H_{1,2,\dots,\tau+t}\} \\ &= \sum_{i=3}^{d-1} \sum_{\mathcal{S} \in \mathcal{U}_i} \mathbf{l}\{\mathcal{S} \text{ is not covered by } H_{\tau+1,\tau+2,\dots,\tau+t}\}. \end{aligned}$$

Then, the expected value of ξ is

$$\sum_{i=3}^{d-1} \sum_{\mathcal{S} \in \mathcal{U}_i} \mathbb{P}\{\mathcal{S} \text{ is not covered by } H_{\tau+1,\tau+2,\dots,\tau+t}\} \quad (2)$$

To find the probabilities in (2), recall (cf. [13, p. 139]) that $2^r \times n$ matrix, consisting of all codewords of \mathcal{C}^\perp , is an orthogonal array of strength $d-1$. This means that for any $i = 3, 4, \dots, d-1$, the projection of this matrix on any i -set \mathcal{S} contains every vector of length i exactly 2^{r-i} times. There are exactly $i \cdot 2^{r-i}$ codewords in \mathcal{C}_0^\perp that cover \mathcal{S} . Therefore,

$$\begin{aligned} \mathbb{P}\{\mathcal{S} \text{ is not covered by } H_{\tau+1,\tau+2,\dots,\tau+t}\} \\ = \frac{\binom{(2^r - \tau - 1) - i \cdot 2^{r-i}}{t}}{\binom{2^r - \tau - 1}{t}} \\ = \prod_{j=\tau+1}^{\tau+t} \left(1 - \frac{i \cdot 2^{r-i}}{2^r - j} \right). \end{aligned} \quad (3)$$

In a numerator we have a number of possible choices of $\mathbf{h}_{\tau+1}, \mathbf{h}_{\tau+2}, \dots, \mathbf{h}_{\tau+t}$ that do not cover \mathcal{S} , and in a denominator – the total number of choices of $\mathbf{h}_{\tau+1}, \mathbf{h}_{\tau+2}, \dots, \mathbf{h}_{\tau+t}$.

By substituting expression (3) into (2) we have that the expected value of ξ is bounded from above by:

$$\mathbb{E}\{\xi\} \leq \sum_{i=3}^{d-1} u_i \prod_{j=\tau+1}^{\tau+t} \left(1 - \frac{i \cdot 2^{r-i}}{2^r - j} \right). \quad (4)$$

Next, it was shown in [9, Lemma 6] that if we draw uniformly at random s codewords from \mathcal{C}^\perp , $s \geq r$, then the matrix constructed from these codewords has expected rank at least

$$r - \frac{1}{2^{s-r}} \left(1 + \frac{2/3}{2^{s-r+1} - 1} \right).$$

It is easy to see that if we draw $\mathbf{h}_{\tau+1}, \mathbf{h}_{\tau+2}, \dots, \mathbf{h}_{\tau+t}$ uniformly at random from $\mathcal{C}_0^\perp \setminus \{\mathbf{h}_1, \mathbf{h}_2, \dots, \mathbf{h}_\tau\}$, and then construct the matrix $H_{1,2,\dots,\tau+t}$, then the expected value of its rank deficiency is bounded from above:

$$\begin{aligned} \mathbb{E}\{\eta\} &= r - \mathbb{E}\{\text{rank } H_{1,2,\dots,\tau+t}\} \\ &\leq \frac{1}{2^{t-r}} \left(1 + \frac{2/3}{2^{t-r+1} - 1} \right). \end{aligned} \quad (5)$$

By summing up (4) and (5), we obtain that

$$\begin{aligned} \mathbb{E}\{\delta(H_{1,2,\dots,\tau+t})\} &\leq \sum_{i=3}^{d-1} u_i \prod_{j=\tau+1}^{\tau+t} \left(1 - \frac{i \cdot 2^{r-i}}{2^r - j} \right) \\ &\quad + \frac{1}{2^{t-r}} \left(1 + \frac{2/3}{2^{t-r+1} - 1} \right). \end{aligned}$$

Since $\delta(H_{1,2,\dots,\tau+t})$ is an integer discrete random variable, there is a realisation of it such that

$$\delta(H_{1,2,\dots,\tau+t}) \leq \left[\sum_{i=3}^{d-1} u_i \prod_{j=\tau+1}^{\tau+t} \left(1 - \frac{i \cdot 2^{r-i}}{2^r - j} \right) + \frac{1}{2^{t-r}} \left(1 + \frac{2/3}{2^{t-r+1} - 1} \right) \right].$$

Step 2. At this point we consider $\mathbf{h}_1, \mathbf{h}_2, \dots, \mathbf{h}_{\tau+t}$ as non-random and fixed. In particular, ξ and η are non-random. Let $\mathcal{U} \subset \mathcal{I}$ be the set of all i -sets ($3 \leq i \leq d-1$) not covered by $H_{1,2,\dots,\tau+t}$. Add one more new row $\mathbf{h}_{\tau+t+1}$, which is randomly chosen from $\mathcal{C}_0^\perp \setminus \{\mathbf{h}_1, \mathbf{h}_2, \dots, \mathbf{h}_{\tau+t}\}$. Analogously to ξ and η for $H_{1,2,\dots,\tau+t}$, we define discrete random variables ξ' and η' for $H_{1,2,\dots,\tau+t+1}$. Then,

$$\begin{aligned} \mathbb{E}\{\xi'\} &= \sum_{\mathcal{S} \in \mathcal{U}} \mathbb{P}\{\mathcal{S} \text{ is not covered by } H_{1,2,\dots,\tau+t+1}\} \\ &\leq |\mathcal{U}| \cdot \max_{\mathcal{S} \in \mathcal{U}} \mathbb{P}\{\mathcal{S} \text{ is not covered by } \mathbf{h}_{\tau+t+1}\} \\ &= \xi \cdot \max_{\mathcal{S} \in \mathcal{U}} \left(1 - \frac{|\mathcal{S}| \cdot 2^{r-|\mathcal{S}|}}{2^r - (\tau+t+1)} \right) \\ &\leq \xi \left(1 - \frac{(d-1) \cdot 2^{r-d+1}}{2^r - (\tau+t+1)} \right). \end{aligned}$$

Adding one row to any matrix could either leave its rank unchanged or increase it by one. Therefore, if $\eta \geq 1$ then¹ we have that either $\eta' = \eta$ or $\eta' = \eta - 1$. To calculate the probabilities of these events, we note that any l linearly independent rows in \mathcal{C}_0^\perp span in total 2^l codewords (including $\mathbf{0}$). Then

$$\mathbb{P}\{\eta' = \eta\} = \frac{2^{r-\eta} - (\tau+t+1)}{2^r - (\tau+t+1)} = 1 - \mathbb{P}\{\eta' = \eta - 1\},$$

and, therefore,

$$\mathbb{E}\{\eta'\} = \eta - \left(\frac{2^r - 2^{r-\eta}}{2^r - (\tau+t+1)} \right).$$

Next, apply Lemma 1 with $b = \eta$ and $x = \tau+t+1$. Indeed, $\eta \geq 1$ and $\eta \leq r-2$ because $H_{1,2,\dots,\tau+t}$ consists of at least two different non-zero codewords. Additionally, $\tau+t+1 < 2^r$ since $2^r - 1$ is the maximum number of rows in any parity-check matrix for \mathcal{C} . Therefore,

$$\mathbb{E}\{\eta'\} \leq \eta \left(1 - \frac{(d-1) \cdot 2^{r-d+1}}{2^r - (\tau+t+1)} \right). \quad (6)$$

Inequality (6) holds also when $\eta = 0$ (which includes the case $r = 2$), because in that case $\eta' = 0$ as well.

Altogether we have

$$\begin{aligned} \mathbb{E}\{\delta(H_{1,2,\dots,\tau+t+1})\} &= \mathbb{E}\{\xi'\} + \mathbb{E}\{\eta'\} \\ &\leq \delta(H_{1,2,\dots,\tau+t}) \left(1 - \frac{(d-1) \cdot 2^{r-d+1}}{2^r - (\tau+t+1)} \right). \end{aligned}$$

Therefore, there exists $\mathbf{h}_{\tau+t+1}$ such that $\delta(H_{1,2,\dots,\tau+t+1}) \leq P_1(\delta(H_{1,2,\dots,\tau+t})) \leq P_1(\lfloor \mathcal{D}_t \rfloor)$. We iterate this process of

¹Note that the case $\eta \geq 1$ is possible only for $r \geq 3$.

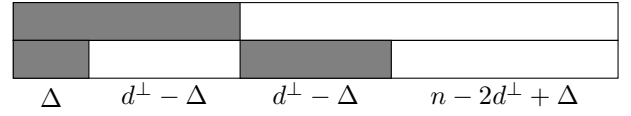


Figure 1. Two codewords of weight d^\perp

adding rows one-by-one, and after k steps obtain the $(\tau + t + k) \times n$ matrix $H_{1,2,\dots,\tau+t+1}$ with $\delta(H_{1,2,\dots,\tau+t+1}) \leq Q_k(\lfloor \mathcal{D}_t \rfloor)$.

Iterations should be stopped when $Q_k(\lfloor \mathcal{D}_t \rfloor) = 0$. ■

III. IMPORTANT SPECIAL CASES

Theorem 1 gives a general family of bounds on the stopping redundancy. It remains a question how to choose particular τ and $\mathbf{h}_1, \mathbf{h}_2, \dots, \mathbf{h}_\tau$, which yield good concrete bounds. In this section, we study specific selections of these parameters.

The first and simple choice is to take $\tau = 1$ and \mathbf{h}_1 to be a fixed codeword of the minimum weight in d^\perp .

Corollary 1. *The upper bound in Theorem 1 holds for $\tau = 1$ and*

$$u_i = \binom{n}{i} - d^\perp \binom{n-d^\perp}{i-1} \text{ for } i = 3, 4, \dots, d-1.$$

Proof: Matrix consisting of one codeword of weight d^\perp covers exactly $d^\perp \binom{n-d^\perp}{i-1}$ i -sets for each $i = 3, 4, \dots, d-1$. We apply Theorem 1 with $\tau = 1$ and $u_i = \binom{n}{i} - d^\perp \binom{n-d^\perp}{i-1}$, which yields the result stated in the corollary. ■

Next, take $\tau = 2$ and consider two different codewords of weight d^\perp .

Corollary 2. *If there are at least two different codewords $\mathbf{h}_1, \mathbf{h}_2 \in \mathcal{C}^\perp$ of weight d^\perp , then the upper bound in Theorem 1 holds for $\tau = 2$, where*

$$\begin{aligned} u_i &= \binom{n}{i} - \mathfrak{M}(n, d^\perp, i), \\ \mathfrak{M}(n, d^\perp, i) &\triangleq 2d^\perp \binom{n-d^\perp}{i-1} - \max_{0 \leq \Delta \leq \lfloor d^\perp/2 \rfloor} \left\{ \Delta \cdot \right. \\ &\quad \left. \binom{n-2d^\perp+\Delta}{i-1} + (\Delta-d^\perp)^2 \binom{n-2d^\perp+\Delta}{i-2} \right\}. \end{aligned}$$

Proof: Consider two different codewords in \mathcal{C}_0^\perp of weight d^\perp . They are shown in Figure 1, where grey and white colors denote the regions of ones and zeroes, respectively. Let Δ be the number of codeword positions, where both of the codewords have ones. Obviously $0 \leq \Delta \leq \lfloor d^\perp/2 \rfloor$.

Each of the codewords covers exactly $d^\perp \binom{n-d^\perp}{i-1}$ i -sets. To calculate the total number of i -sets covered by these two codewords we need to subtract those i -sets that have been counted twice. They are of two kinds:

- Covered by the same pattern of size i in \mathbf{h}_1 and \mathbf{h}_2 . They have one position in the area of length Δ and all the other positions in the area of length $n - 2d^\perp + \Delta$. There are $\Delta \binom{n-2d^\perp+\Delta}{i-1}$ such i -sets.

- Covered by different patterns of size i (at the same positions) in \mathbf{h}_1 and \mathbf{h}_2 . They have one position in each of areas of length $d^\perp - \Delta$ and the remaining $i - 2$ positions in the area of length $n - 2d^\perp + \Delta$. There are $(\Delta - d^\perp)^2 \binom{n - 2d^\perp + \Delta}{i - 2}$ such i -sets.

Therefore these two codewords cover together the following amount of i -sets

$$2d^\perp \binom{n - d^\perp}{i - 1} - \Delta \binom{n - 2d^\perp + \Delta}{i - 1} - (\Delta - d^\perp)^2 \binom{n - 2d^\perp + \Delta}{i - 2}.$$

This is at least $\mathfrak{M}(n, d^\perp, i)$. We can now apply Theorem 1 with $\tau = 2$ and $u_i = \binom{n}{i} - \mathfrak{M}(n, d^\perp, i)$. ■

It might be possible to further improve the bound in Corollary 2 by judiciously selecting three or more codewords in \mathcal{C}^\perp , for example by taking three (or more) dual codewords of weight d^\perp . However, in that case it becomes more difficult to obtain good analytical estimates on u_i . Alternatively, it is also possible to choose some specific $\mathbf{h}_1, \mathbf{h}_2, \dots, \mathbf{h}_\tau$ and to compute all u_i directly by computer. In that case, tighter bounds can be obtained. In the sequel, we refer to that method as a *hybrid method*.

IV. STOPPING REDUNDANCY HIERARCHY

Consider a binary $[n, k, d]$ code \mathcal{C} . In Definition 2 it is required that the stopping distance of the code defined by the parity-check matrix H is d . However, a weaker requirement on the parity-check matrix of the code can be imposed. In this section, as it was suggested in [8], we require that the stopping distance of the code is at least l , for some $1 \leq l \leq d$. In that case, the number of rows in the parity-check matrix can be smaller than the stopping redundancy of the code.

Definition 3 ([8, Definition 2.4]). *For $l \leq d$, the l -th stopping redundancy of \mathcal{C} is the smallest nonnegative integer $\rho_l(\mathcal{C})$ such that there exists a (possibly redundant) parity-check matrix H of \mathcal{C} with $\rho_l(\mathcal{C})$ rows and stopping distance at least l . The ordered set of integers $(\rho_1(\mathcal{C}), \rho_2(\mathcal{C}), \dots, \rho_d(\mathcal{C}))$ is called the stopping redundancy hierarchy of \mathcal{C} .*

Note that the (conventional) stopping redundancy $\rho(\mathcal{C})$ is equal to $\rho_d(\mathcal{C})$. For codes with the minimum distance $d \geq 4$, neither two columns of the parity-check matrix are identical nor any of the columns equal to the all-zero vector. Therefore, $\rho_1(\mathcal{C}) = \rho_2(\mathcal{C}) = \rho_3(\mathcal{C}) = n - k$. Consequently, only $\rho_l(\mathcal{C})$ for $l > 3$ is of interest.

In [8], the stopping redundancy hierarchy of binary linear codes is studied, and several upper bounds are obtained. In the sequel, we apply the ideas in previous section to the stopping redundancy hierarchy. We formulate a generalised version of Corollary 2.

Theorem 2. *If \mathcal{C}^\perp contains at least two codewords of minimum weight d^\perp , then for $4 \leq l \leq d$,*

$$\rho_l(\mathcal{C}) \leq 2 + \min_{t \geq r} \left\{ t + \kappa_t^{(1)} \right\} + (r - l + 1).$$

Moreover, if $(r - 1)(l - 1) \leq 2^{l-1}$ then

$$\rho_l(\mathcal{C}) \leq 2 + \min_{t \geq r} \left\{ t + \kappa_t^{(2)} \right\},$$

where

$$\begin{aligned} \kappa_t^{(i)} &= \min \left\{ k \in \mathbb{N} : Q_k(\lfloor \mathcal{D}_t^{(i)} \rfloor) = 0 \right\}, \quad i = 1, 2, \\ Q_k(x) &= P_k(P_{k-1}(\dots P_1(x) \dots)), \\ P_j(x) &= \left\lfloor x \left(1 - \frac{(l-1)2^{r-l+1}}{2^r - (2+t+j)} \right) \right\rfloor, \\ \mathcal{D}_t^{(1)} &= \sum_{i=3}^{l-1} u_i \prod_{j=2}^{t+2} \left(1 - \frac{i \cdot 2^{r-i}}{2^r - j} \right), \\ \mathcal{D}_t^{(2)} &= \mathcal{D}_t^{(1)} + \frac{1}{2^{t-r}} \left(1 + \frac{2/3}{2^{t-r+1} - 1} \right), \\ u_i &= \binom{n}{i} - \mathfrak{M}(n, d^\perp, i). \end{aligned}$$

Proof: The case when $(r - 1)(l - 1) \leq 2^{l-1}$ is analogous to the proof of Theorem 1, with the values of τ and u_i as in Corollary 2.

That proof, however, cannot be applied to the cases of small values of l if the condition $(r - 1)(l - 1) \leq 2^{l-1}$ does not hold. We note that this condition is required in the proof only to guarantee the uniform decrease of ξ and η . Therefore, the argument for decrease of ξ in the proof of Theorem 1 can be applied as is. After that, we have to ensure that the constructed matrix is of the required rank r .

Note that since we have covered all the i -sets for $i = 1, 2, \dots, l - 1$, the rank of the matrix is at least $l - 1$. Hence, by adjoining at most $r - (l - 1)$ rows, we finally obtain the required parity-check matrix. ■

We note that tighter bounds on the stopping redundancy hierarchy could be obtained by using the hybrid method, discussed in the last paragraph of Section III.

V. NUMERICAL EXPERIMENTS

In this section, we compare the bounds on the stopping redundancy obtained in [3], [6], [9] with our results. We consider two codes: the extended [24, 12, 8] binary Golay code and the extended [48, 24, 12] binary Quadratic Residue (QR) code. Both of them are known to be self-dual (cf. [14]).

The extended [24, 12, 8] binary Golay code is arguably a remarkable binary block code. It is often used as a benchmark in studies of code structure and decoding algorithms. The code is self-dual, therefore $d^\perp = 8$. Moreover, it is known [13, p. 67] that there are 759 codewords of the minimum weight. The example of (conventional) parity-check matrix of the code is shown in Table I, where the blank spaces denote zeroes. In [3], a greedy (lexicographic) computer search was used. It was found that the actual stopping redundancy of the extended [24, 12, 8] binary Golay code is at most 34.

It is known [13, p. 604] that there are 17296 codewords of the minimum weight in the extended [48, 24, 12] binary Quadratic Residue (QR) code. The comparison of the upper bounds on the stopping redundancy is given in Table II.

PARITY-CHECK MATRIX OF THE EXTENDED $[24, 12, 8]$ GOLAY CODE

[illegible]

Table II
UPPER BOUNDS ON THE STOPPING REDUNDANCY

	[24, 12, 8] Golay	[48, 24, 12] QR
[3, Thm 4]	2509	4540385
[9, Thm 1]	198	3655
[9, Thm 3]	194	3655
[9, Thm 4]	187	3577
[9, Thm 7]	182	3564
Corollary 1 ($\tau = 1$)	180	3538
Corollary 2 ($\tau = 2$)	177	3515

We also compare the bounds on stopping redundancy hierarchy in the previous chapter with the results for general codes, obtained in [8] (the bounds for cyclic codes therein are not applicable because neither of the codes is cyclic.) The numerical results are presented in Table III and Table IV.

Next, we use the hybrid method, mentioned in the last paragraph of Section III. We take τ first rows of conventional parity-check matrix of the extended $[24, 12, 8]$ Golay code (Table I), for $1 \leq \tau \leq 12$, compute all u_i , and apply techniques similar to Theorem 1 and Theorem 2. Numerical results are presented in Table V.

Table III
BOUNDS ON THE STOPPING REDUNDANCY HIERARCHY, ρ_l , FOR THE
EXTENDED $[24, 12, 8]$ GOLAY CODE

l	[8, Thm 3.8]	[8, Thm 3.11]	[8, Thm 3.12]	Thm 2
4	26	78	—	25
5	—	298	—	36
6	—	793	385	59
7	—	1585	—	103
8	—	2509	—	177

Table IV
BOUNDS ON THE STOPPING REDUNDANCY HIERARCHY, ρ_i , FOR THE
EXTENDED [48, 24, 12] QR CODE

l	[8, Thm 3.8]	[8, Thm 3.11]	Thm 2
4	42	300	47
5	62	2 324	58
6	105	12 950	92
7	—	55 454	158
8	—	190 050	287
9	—	536 154	514
10	—	1 271 625	978
11	—	2 579 129	1856
12	—	4 540 385	3515

Table V
BOUNDS ON THE STOPPING REDUNDANCY HIERARCHY, ρ_l , DERIVED BY
THE HYBRID METHOD FOR THE EXTENDED [24, 12, 8] GOLAY CODE

ρ_l	$l = 4$	$l = 5$	$l = 6$	$l = 7$	$l = 8$
$\tau = 1$	24	36	61	105	180
$\tau = 2$	24	36	59	103	177
$\tau = 3$	25	35	58	102	175
$\tau = 4$	25	34	57	100	174
$\tau = 5$	26	33	56	99	172
$\tau = 6$	27	33	56	98	171
$\tau = 7$	28	33	55	98	170
$\tau = 8$	29	33	55	97	169
$\tau = 9$	30	33	55	96	168
$\tau = 10$	31	33	55	96	167
$\tau = 11$	32	34	55	96	167
$\tau = 12$	33	35	56	97	168

VI. ACKNOWLEDGMENT

The authors wish to thank Øyvind Ytrehus for helpful discussions.

REFERENCES

- [1] C. Di, D. Proietti, I. E. Telatar, T. J. Richardson, and R. L. Urbanke, "Finite-length analysis of low-density parity-check codes on the binary erasure channel," *IEEE Trans. Inf. Theory*, vol. 48, no. 6, pp. 1570–1579, 2002.
- [2] N. Santhi and A. Vardy, "On the effect of parity-check weights in iterative decoding," in *Proc. IEEE Intern. Symp. on Information Theory*, 2004, p. 322.
- [3] M. Schwartz and A. Vardy, "On the stopping distance and the stopping redundancy of codes," *IEEE Trans. Inf. Theory*, vol. 52, no. 3, pp. 922–932, 2006.
- [4] J. H. Weber and K. A. Abdel-Ghaffar, "Stopping set analysis for Hamming codes," in *Proc. Inform. Theory Workshop*, 2005, pp. 244–247.
- [5] T. Etzion, "On the stopping redundancy of Reed-Muller codes," *IEEE Trans. Inf. Theory*, vol. 52, no. 11, pp. 4867–4879, 2006.
- [6] J. Han and P. H. Siegel, "Improved upper bounds on stopping redundancy," *IEEE Trans. Inf. Theory*, vol. 53, no. 1, pp. 90–104, 2007.
- [7] H. D. Hollmann and L. M. Tolhuizen, "On parity-check collections for iterative erasure decoding that correct all correctable erasure patterns of a given size," *IEEE Trans. Inf. Theory*, vol. 53, no. 2, pp. 823–828, 2007.
- [8] T. Hehn, O. Milenkovic, S. Laendner, and J. B. Huber, "Permutation decoding and the stopping redundancy hierarchy of cyclic and extended cyclic codes," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5308–5331, 2008.
- [9] J. Han, P. H. Siegel, and A. Vardy, "Improved probabilistic bounds on stopping redundancy," *IEEE Trans. Inf. Theory*, vol. 54, no. 4, pp. 1749–1753, 2008.
- [10] J. Zumbärgel, V. Skachek, and M. F. Flanagan, "On the pseudocodeword redundancy of binary linear codes," *IEEE Trans. Inf. Theory*, vol. 58, no. 7, pp. 4848–4861, 2012.
- [11] E. Rosnes and Ø. Ytrehus, "An efficient algorithm to find all small-size stopping sets of low-density parity-check matrices," *IEEE Trans. Inf. Theory*, vol. 55, no. 9, pp. 4167–4178, 2009.
- [12] M. Karimi and A. H. Banihashemi, "Efficient algorithm for finding dominant trapping sets of LDPC codes," *IEEE Trans. Inf. Theory*, vol. 58, no. 11, pp. 6942–6958, 2012.
- [13] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*. Elsevier, 1977.
- [14] S. K. Houghten, C. W. Lam, L. H. Thiel, and J. A. Parker, "The extended quadratic residue code is the only (48, 24, 12) self-dual doubly-even code," *IEEE Trans. Inf. Theory*, vol. 49, no. 1, pp. 53–59, 2003.